(12) UK Patent Application (19) GB (11) 2 363 284 (13) A

(43) Date of A Publication 12.12.2001

(21) Application No 0100126.2

(22) Date of Filing 03.01.2001

(30) Priority Data
(31) 09479206 (32) 07.01.2000 (33) US

(71) Applicant(s)
Hewlett-Packard Company
(Incorporated in USA - Delaware)
3000 Hanover Street, Palo Alto, California 94304,
United States of America

(72) Inventor(s)
Jason D Goldman
Bogunia E Pawlak
Robert C Vacante
Evelyn L Williams

(74) Agent and/or Address for Service
Carpmaels & Ransford
43 Bloomsbury Square, LONDON, WC1A 2RA,
United Kingdom

(51) INT CL[7]
H04Q 3/00

(52) UK CL (Edition S)
H4K KFMA

(56) Documents Cited
GB 2356316 A GB 2337409 A

(58) Field of Search
UK CL (Edition S) H4K KFMA KF42
INT CL[7] H04Q 3/00
Online:WPI,JAPIO,EPODOC

(54) Abstract Title
Two-stage deployment of policy to a communications network element

(57) As used herein, a "policy" means the combination of one or more rules assigned to a network element or elements. A policy typically contains one or more rules defining the conditions for provision or denial of bandwidth or priority. It is known that a network element may be programmed with a policy which is rejected due to inconsistencies in the policy or the condition of the network. To overcome this problem, an extra deployment stage is used wherein policies can be created, tested, changed or deleted prior to their transfer to the network elements. The extra deployment stage permits these functions to be performed at a single location.

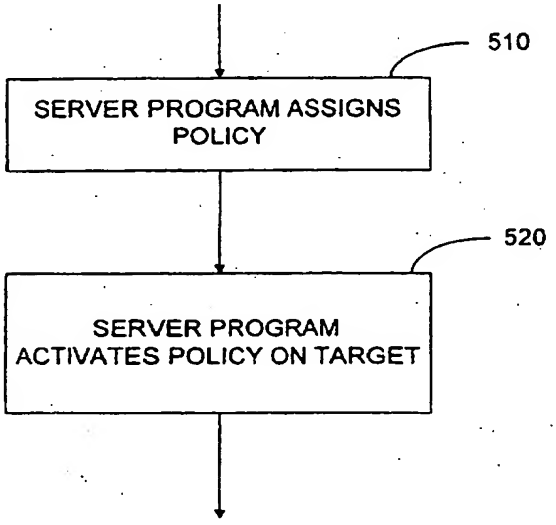

FIG.5A

GB 2 363 284 A

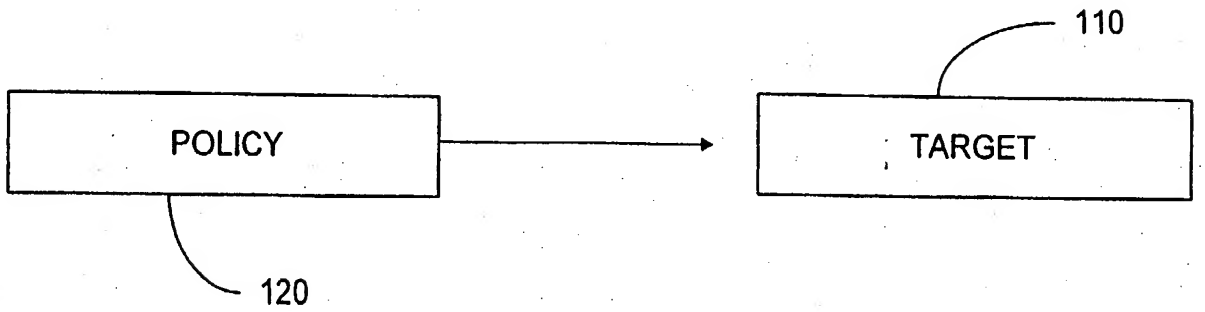

FIG.1

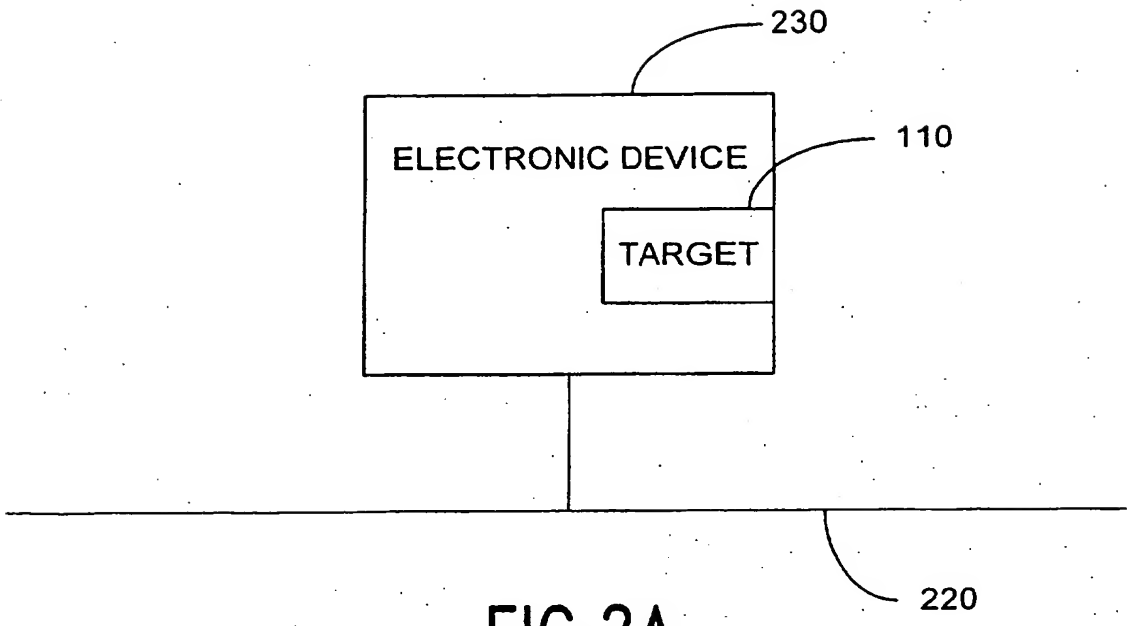
230
ELECTRONIC DEVICE
110
TARGET
220

FIG.2A

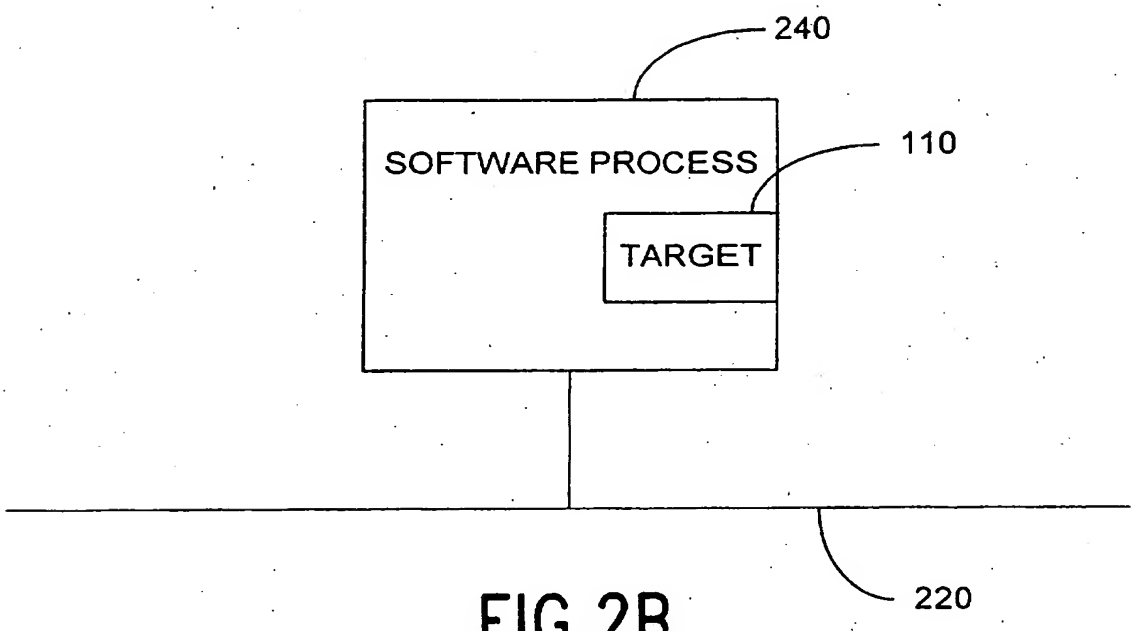
240
SOFTWARE PROCESS
110
TARGET
220

FIG.2B

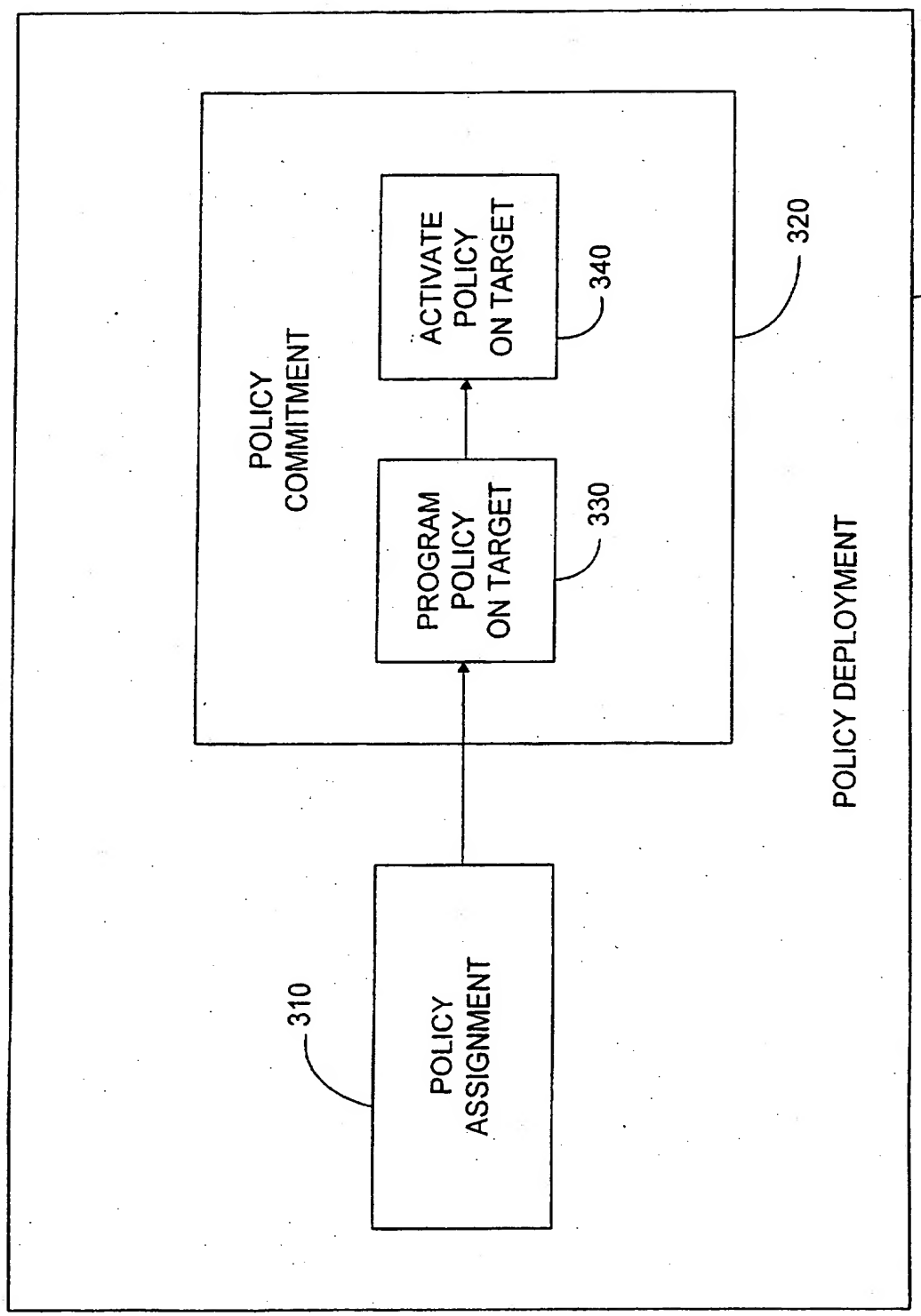
POLICY DEPLOYMENT
300
POLICY COMMITMENT
320
ACTIVATE POLICY ON TARGET
340
PROGRAM POLICY ON TARGET
330
POLICY ASSIGNMENT
310

FIG.3

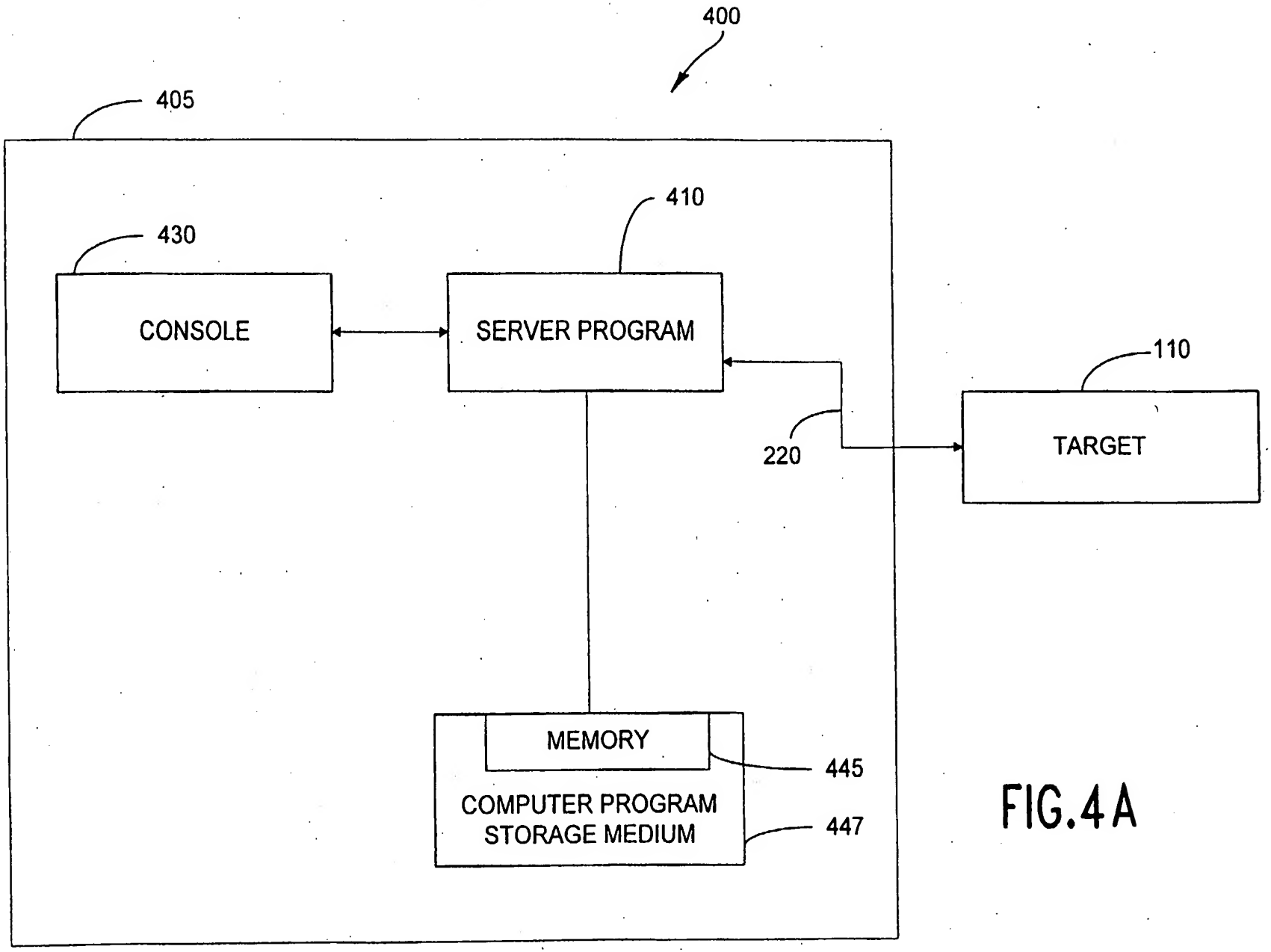
400
405
410
430
CONSOLE
SERVER PROGRAM
110
220
TARGET
MEMORY
445
COMPUTER PROGRAM
STORAGE MEDIUM
447

FIG.4A

4/10

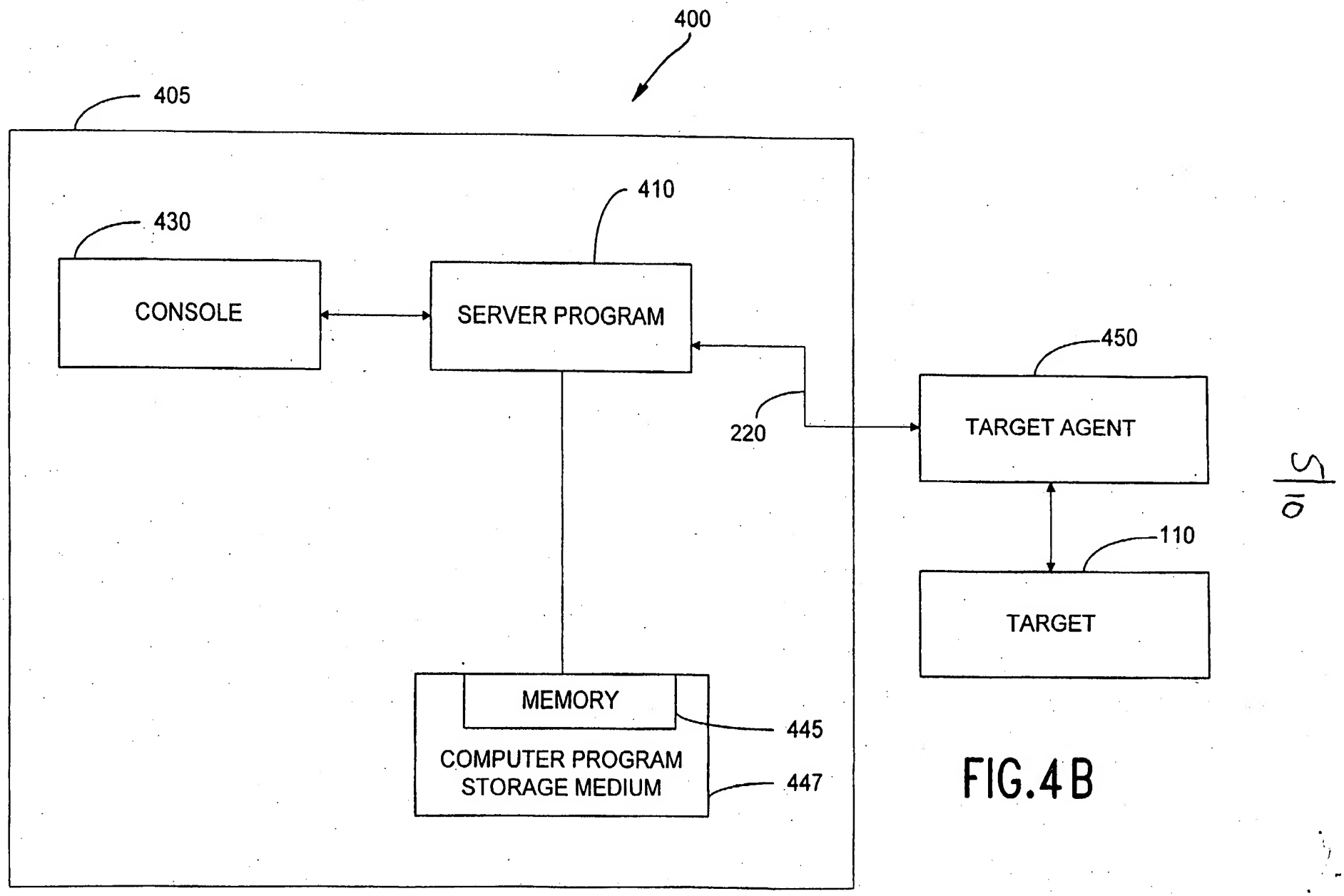
400
405
410
430
CONSOLE
SERVER PROGRAM
450
220
TARGET AGENT
110
TARGET
MEMORY
445
COMPUTER PROGRAM
STORAGE MEDIUM
447

FIG.4B

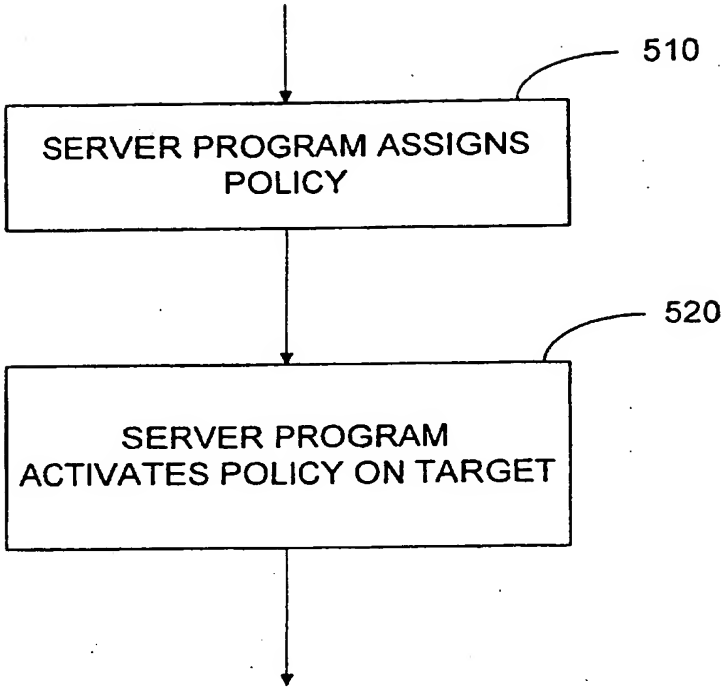
510
SERVER PROGRAM ASSIGNS POLICY
520
SERVER PROGRAM ACTIVATES POLICY ON TARGET

FIG.5A

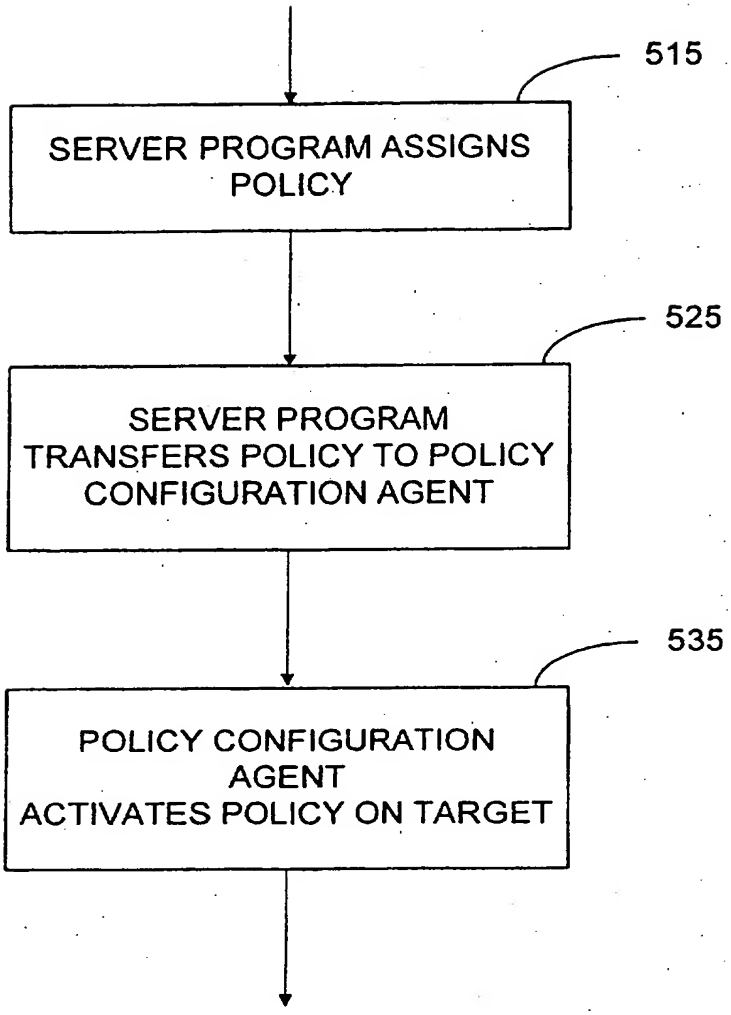
515
SERVER PROGRAM ASSIGNS POLICY
525
SERVER PROGRAM TRANSFERS POLICY TO POLICY CONFIGURATION AGENT
535
POLICY CONFIGURATION AGENT ACTIVATES POLICY ON TARGET

FIG.5B

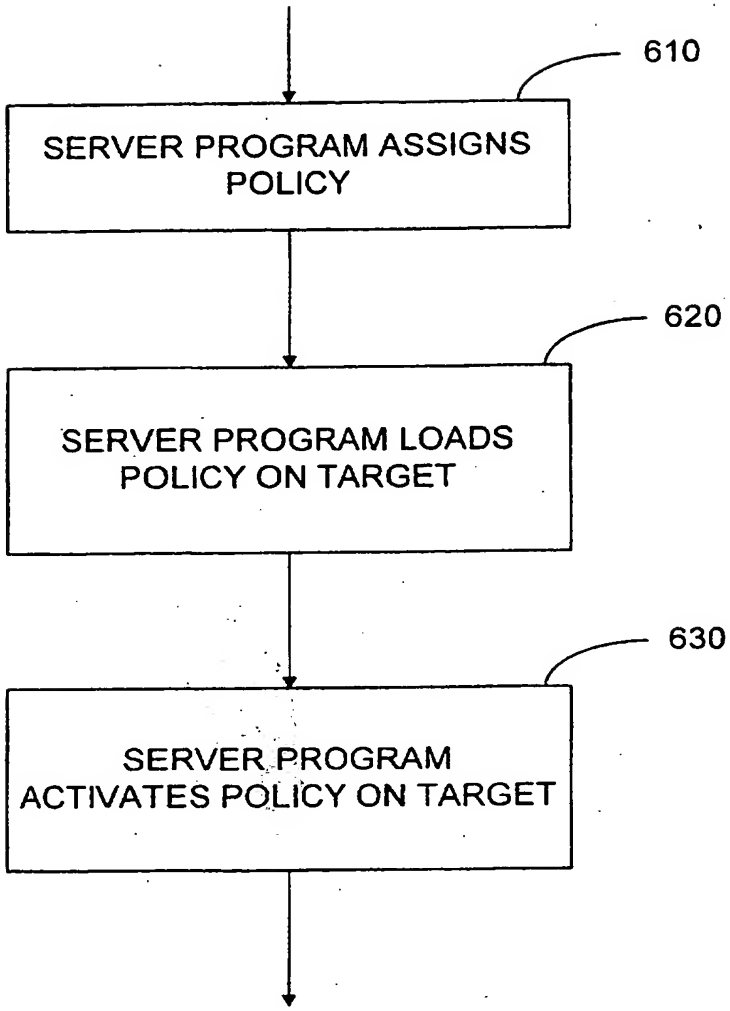
610
SERVER PROGRAM ASSIGNS POLICY
620
SERVER PROGRAM LOADS POLICY ON TARGET
630
SERVER PROGRAM ACTIVATES POLICY ON TARGET

FIG.6A

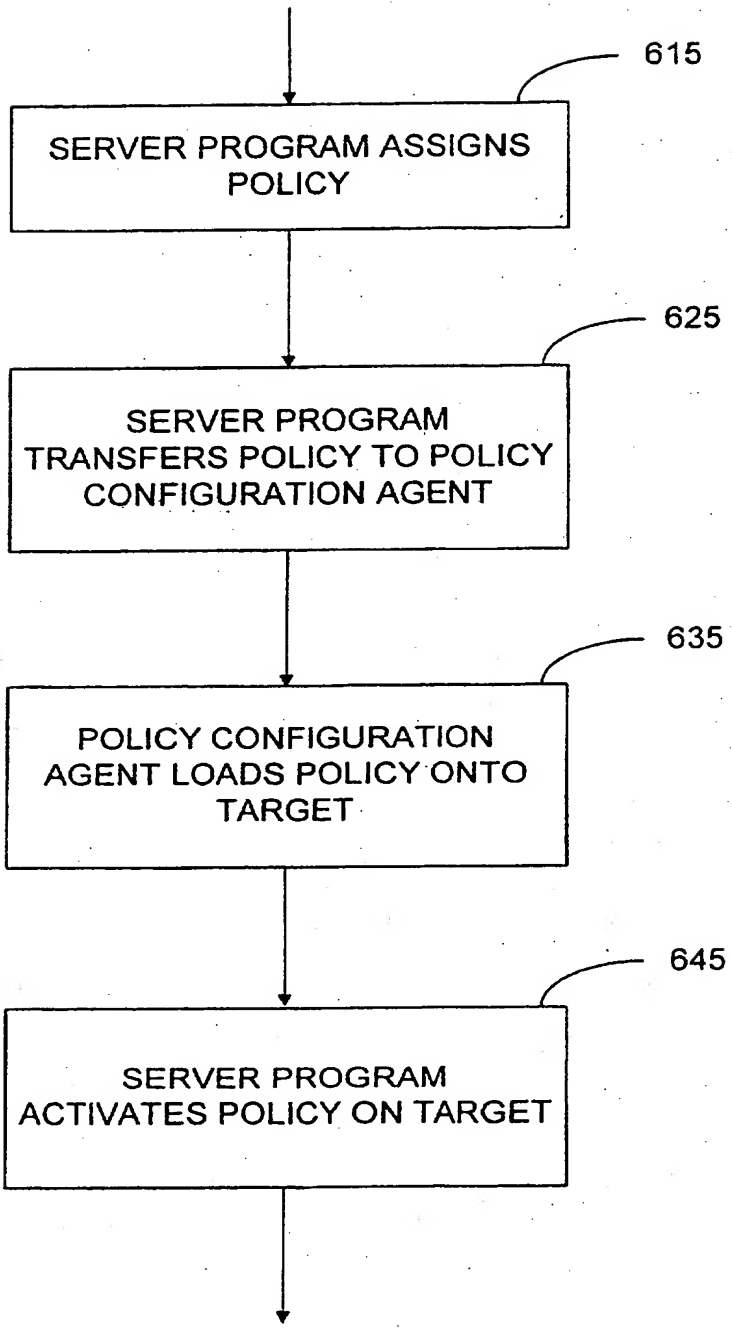
615
SERVER PROGRAM ASSIGNS POLICY
625
SERVER PROGRAM TRANSFERS POLICY TO POLICY CONFIGURATION AGENT
635
POLICY CONFIGURATION AGENT LOADS POLICY ONTO TARGET
645
SERVER PROGRAM ACTIVATES POLICY ON TARGET

FIG.6B

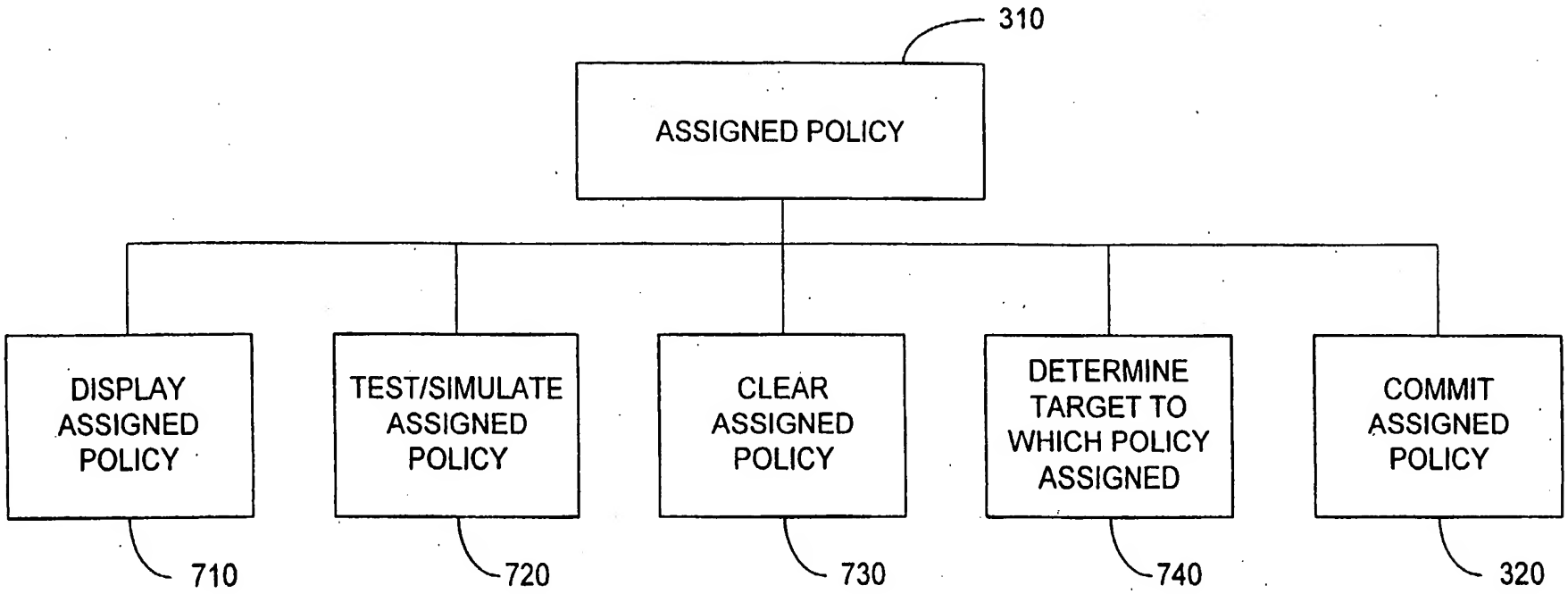
310
ASSIGNED POLICY
DISPLAY ASSIGNED POLICY
TEST/SIMULATE ASSIGNED POLICY
CLEAR ASSIGNED POLICY
DETERMINE TARGET TO WHICH POLICY ASSIGNED
COMMIT ASSIGNED POLICY
710
720
730
740
320

FIG.7

STAGED DEPLOYMENT OF POLICY IN POLICY-BASED NETWORK MANAGEMENT SYSTEMS

FIELD OF THE INVENTION

The present invention relates generally to networks, more particularly to network management, and even more particularly to policy-based network management.

BACKGROUND OF THE INVENTION

The purpose of policy-based network management is to coordinate device management across an entity's network to enforce policies relating to Service Level Agreements (SLAs). SLAs are agreements made between network users and the network provider. Policy is a method of translating those agreements into actions designed to provide the type and level of service agreed upon. The policies describe sets of rules, where a rule specifies a set of conditions and an action to take when the conditions are satisfied. The actions described within a policy's rules generally relate to Quality of Service (QoS) capabilities, e.g. bandwidth allocated or priority assigned to the traffic. By using policy-based network management, a structural format is provided wherein network administrators can avoid the tedious process of individually configuring multiple network devices, e.g., routers and traffic shapers, each of which has its own particular syntax and mapping of QoS actions to device resources. For example, an Access Control List (ACL) maintains a list of network resources which could, among other things, define permissible actions of a port on a router under specified conditions.

As used herein, a policy means the combination of one or more rules assigned to a network component or components. Thus any given component has only one policy

assigned to it, but it may be composed of a number of rules each having their own conditions and resulting actions.

In general, the network administrator uses SLAs to author a set of policies of varying types, determines what enforcement points in the network should enforce these policies, and then deploys the policies to the enforcement points. The enforcement points are the components of the networks that are the targets of the policy.

Deploying policy involves moving the policy onto the target or target configuration agent, translating the policy into target-specific configuration, and loading this configuration. The notion of a two stage commitment has been discussed within two industry standard setting groups, the Distributed Management Task Force Service Level Agreement (DMTF SLA) working group and the Internet Engineering Task Force (IETF) Policy Framework working group. This is the idea that one can load the policy data onto several targets, the first commitment stage, and then trigger or activate all of the targets to reconfigure themselves at the same time, the second commitment stage. This idea allows the network administrator to coordinate changes to a number of targets and avoid the problems of different targets having conflicting configuration because policy on one of them may not have been updated while it had been on another target. DMTF is an industry organization involved in the development, adoption, and unification of management standards and initiatives for desktop, enterprise and Internet environments. The IETF (Internet Engineering Task Force) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture, as well as the smooth operation of the Internet.

While policy commitment in two stages solves the timing issue with respect to policy deployment, other problems remain. In particular, policies may have been programmed into the target which are rejected due to inconsistencies in the policy and other reasons which could be for example associated with the condition of the network. Note that in two stage commitment, actual activation occurs after the target is programmed and may fail.

Thus, there is a need for another step in the policy deployment process within which policies can be created, tested, changed, and deleted prior to their transfer to the

policy configuration agents of the targets to which it is intended that they will eventually be deployed. In addition, it is desirable that this step permit these functions to be performed at a single location for multiple policies and their associated targets.

SUMMARY OF THE INVENTION

The present patent document relates to a novel method for deployment of policy to a target connected to a network for the purpose of controlling the actions of that target based upon certain predefined conditions. In representative embodiments, methods are disclosed for creating another step in the policy deployment process within which policies can be created, tested, changed, and deleted prior to their transfer to the policy configuration agents of the targets to which it is intended that they will eventually be deployed.

Electronic systems, such as networks, that comprise resources or processes can control the interaction of such items by means of Quality of Service (QoS) mechanisms. These mechanisms can be controlled at a higher level of abstraction using rules, which relate an action, i.e., controlling the QoS mechanism, to a set of conditions describing when to apply the rule. The combination of one or more rules for a given device is referred to herein as a policy. The controlled items could be for example processes, functions, abstract objects, or physical electronic devices such as computers, printers, etc. Thus, policy refers to the description of behaviors or actions that are desired for the item to which the policy applies. In network systems, policies are typically associated with items that affect the flow of data on that network. In order to affect that network traffic flow, policies are directed toward or targeted at managed or controlled entities.

As referred to herein, a target is a process or resource that is being managed using policy. The managed item itself may be able to recognize and conform to the policy directly, or may be managed by a proxy which recognizes policy information and converts it to configuration information that the managed entity can recognize and conform to.

Using the concept of targets, a particular capability or rule can be isolated to a single manageable element which has that capability or functions according to the rules of the policy. In this way the administrator can more readily deal with the manner in which network traffic is to be treated at specific points in the network.

The concept of policy deployment is extended to have two steps: policy

assignment and policy commitment. Commitment occurs only after the policy is resident on the target device. In two stage commitment, a first stage comprises the programming of the policy into the target or onto a policy configuration agent, while a second stage comprises the activation of the policy on the target. Prior to activation the policy resides on the target or on the policy configuration agent but is not active in the operation of the target. Following activation, any previous policy is replaced by the activated policy. In one stage commitment, activation of the policy occurs concurrent with the programming of the policy on the target.

While the commitment step may or may not have two stages, as described above, adding an assignment step addresses a different set of concerns. Providing an assignment stage allows users to make an association between a policy and the policy enforcement point, or target, without affecting or committing to changing the active policy on that target. Note that two stage deployment is independent of supporting a two step commitment process.

This association grants two main benefits: (1) users are provided with a forgiving model for changing policy on the target and (2) the policy-based network management system can allow target specific operations on a policy without changing the target's configuration. The first point is that users can safely stage a policy change for the target since the target's configuration is not changed until the user is certain of the change and commits the assigned policy. Users can plan for policy changes that may occur in the future without locking in those changes. They can also see a policy change on one target in the context of other policy changes on other targets before actually changing their network's behavior with respect to Quality of Service (QoS) policy. This process could also integrate with the user's change management process, e.g., review and approve policy changes before committing them. The second benefit mentioned above is that there are target-specific operations that users might want to perform on a particular policy/target pair. One clear example is to validate the policy for a particular target. This validation step is important because a target may support a given policy type and yet not support all possible condition types for that policy type or the given policy may conflict with other exiting target configuration information. If users can validate the policy for the

intended target before committing the policy, they can avoid problems like leaving the target incorrectly configured or un-configured with respect to QoS. Another example of a target-specific operation would be policy simulation.

The policy-based network management system supports a number of operations related to the two stage deployment mechanism comprising the following: (1) assignment of policy to targets on a per target basis which creates and stores the assignment relationship, (2) display of assigned policy, (3) tests and simulation of assigned policy, (4) clearing of assigned policy, (5) identify to which targets a given policy is assigned, and (6) commit an assigned policy to the target.

Primary advantages of the embodiment as described in the present patent document over prior methods for deploying policy is the ability to overcome the problem that policies may be programmed into the target which may be subsequently rejected due to policy inconsistencies and other reasons and the ability to perform target specific operations such as testing and simulation of policy prior to commitment.

Other aspects and advantages of the present invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, illustrating by way of example the principles of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings provide visual representations which will be used to more fully describe the invention and can be used by those skilled in the art to better understand it and its inherent advantages. In these drawings, like reference numerals identify corresponding elements and:

Figure 1 is a drawing showing a policy related to a target as described in various representative embodiments of the present patent document.

Figure 2A is a drawing of the target connected to a network as described in various representative embodiments of the present patent document.

Figure 2B is a drawing of another target connected to the network as described in various representative embodiments of the present patent document.

Figure 3 is a drawing of policy deployment to the target as described in various representative embodiments of the present patent document.

Figure 4A is a drawing of a system for policy management by a server program for the target as described in various representative embodiments of the present patent document.

Figure 4B is a drawing of another system for policy management by the server program for the target as described in various representative embodiments of the present patent document.

Figure 5A is a flow chart of policy deployment to the target with one stage policy commitment as described in various representative embodiments of the present patent document.

Figure 5B is another flow chart of policy deployment to the target with one stage policy commitment as described in various representative embodiments of the present patent document.

Figure 6A is a flow chart of policy deployment to the target with two stage policy commitment as described in various representative embodiments of the present patent document.

Figure 6B is another flow chart of policy deployment to the target with two stage

policy commitment as described in various representative embodiments of the present patent document.

Figure 7 is a drawing of a block diagram of operations that can be performed on the assigned policy.

5

1. Introduction

As shown in the drawings for purposes of illustration, the present patent document relates to a novel method for deployment of policy to a target connected to a network for the purpose of controlling the actions of that target based upon certain predefined conditions. In representative embodiments, the present patent document discloses methods for creating another step in the policy deployment process within which policies can be created, tested, changed, and deleted prior to their transfer to the policy agents of the targets to which it is intended that they will eventually be deployed. In the following detailed description and in the several figures of the drawings, like elements are identified with like reference numerals.

2. Policies

Electronic systems, such as networks, that comprise resources or processes can control the interaction of such items by means of Quality of Service (QoS) mechanisms. These mechanisms can be controlled at a higher level of abstraction using rules, which relate an action, i.e., controlling the QoS mechanism, to a set of conditions describing when to apply the rule. The combination of one or more rules for a given device is referred to herein as a policy. The controlled items could be for example processes, functions, abstract objects, or physical electronic devices such as computers, printers, etc. Thus, policy refers to the description of behaviors or actions that are desired for the item to which the policy applies. In network systems, policies are typically associated with items that affect the flow of data on that network. In order to affect that network traffic flow, policies are directed toward or targeted at managed or controlled entities. An example of a policy could be "assign priority 5 to traffic from the user whose name is user_one".

3. Targets

Figure 1 is a drawing showing a policy **120** related to a target **110** as described in various representative embodiments of the present patent document. As referred to herein, the target **110** is a process or resource that is being managed using policy **120**. The managed item itself may be able to recognize and conform to the policy **120**, or may be managed by a proxy which recognizes policy **120** information and converts it to configuration information that the managed entity can recognize and conform to.

Modern network devices are typically managed as a unit, i.e., the various features of the device are all managed together. For example, a router has multiple interfaces, with each interface representing a connection to one or more networks. The router's function is to route traffic between these networks. Further, each interface can have multiple capabilities, each of which can affect the traffic in different ways. These mechanisms can each be configured separately. But, in modern network devices all of these different aspects of a single device are typically managed together, usually presenting a difficult to understand interface to the administrator of the network. As a result, the management of even a single device can become a daunting task. In representative embodiments, the present patent document discloses techniques by which policy **120** can be deployed in order to manage separate aspects of specified devices, i.e., targets **110**.

Figure 2A is a drawing of the target **110** connected to a network **220** as described in various representative embodiments of the present patent document. In the example of Figure 2A, the target **110** is a controllable entity of an electronic device **230** which is connected to the network **220**. Using the concept of the target **110**, a particular capability or rule can be isolated to a single manageable element which has that capability or functions according to the rules of the policy. In this way the administrator can more readily deal with the manner in which network traffic is to be treated at specific points in the network.

In the above example, the router could be the electronic device **230** and could also be the target **110**. Alternatively, any interface of the electronic device **230**, which in this example is any interface of the router, could be the target **110**. In another example, the target **110** on the router could also be the priority queuing of messages on a specific

Figure 2B is a drawing of another [illegible]

described in various representative embodiments of the present patent document. In the example of Figure 2B, the target **110** is a controllable entity of a software process **240** which is connected to the network **220**. Again using the concept of the target **110**, a particular capability can be isolated to a single manageable function within the software process **240** which has the specified capability or functions according to the rules of the policy.

Breaking such capabilities into separate conceptual targets **110** of policy **120**, as in the example of the interfaces of the router, enables the same description of behavior to be applied to many different devices which, in a high-level abstraction, provide similar capabilities. In addition, with the appropriate abstractions, devices from different vendors, and indeed different types of devices, e.g., routers, switches, and traffic shapers can be managed with identical policies **120**. Traffic shapers are a class of devices that regulate or shape the flow of network traffic based on a histogram of such traffic.

Thus, the concept of targets **110** can be abstracted down to a discreet function of the smallest manageable item on the single electronic device **230** or system, thereby providing the capability for efficient, simplified, large-scale management of the network **220** with policies **120**.

4. Target Deployment

Figure 3 is a drawing of policy deployment **300** to the target **110** as described in various representative embodiments of the present patent document. The concept of policy deployment **300** is extended to have two steps: policy assignment **310** and policy commitment **320**. Commitment **320** occurs only after the policy is resident on the target device. In two stage commitment, a first stage **330** comprises the programming of the policy into the target **110**, while a second stage **340** comprises the activation of the policy **120** on the target **110**. Prior to activation the policy **120** resides on the target **110** but is not active in the operation of the target **110**. Following activation, any previous policy **120** is replaced by the activated policy **120**. In one stage commitment, activation of the

policy 120 occurs concurrent with the programming of the policy 120 on the target 110.

While the commitment step 320 may or may not have two stages 330,340, as described above, adding assignment step 310 addresses a different set of concerns. Providing assignment stage 310 allows users to make an association between a policy and the policy enforcement point 110, or target 110, without affecting or committing to changing the active policy on that target 110.

This association grants two main benefits: (1) users are provided with a forgiving model for changing policy 120 on the target 110 and (2) the policy-based network management system can allow target 110 specific operations on a policy without changing the target's 110 configuration. The first point is that users can safely stage policy 120 change for the target 110 since the target's 110 configuration is not changed until the user is certain of the change and commits the assigned policy. Users can plan for policy 120 changes that may occur in the future without locking in those changes. They can also see policy 120 change on one target 110 in the context of other policy 120 changes on other targets 110 before actually changing their network's 220 behavior with respect to Quality of Service (QoS) policy. This process could also integrate with the user's change management process, e.g., review and approve policy 120 changes before committing them. The second benefit mentioned above is that there are target-specific operations that users might want to perform on a particular policy/target pair. One clear example is to validate the policy 120 for a particular target 110. This validation step is important because the target 110 may support a given policy 120 type and yet not support all possible condition types for that policy 120 type or the given policy 120 may conflict with other exiting target 110 configuration information. If users can validate the policy 120 for the intended target 110 before committing the policy 120, they can avoid problems like leaving the target 110 incorrectly configured or un-configured with respect to QoS. Another example of a target-specific operation would be to simulate network 220 operation with given policies 120 implemented on targets 110 attached to the network 220.

As can be observed in Figure 3, two stage deployment is independent of supporting a two step commitment process. In fact the two ideas can coexist well

together. In two stage commitment, the new policy is moved onto the target **110** and translated into configuration changes. Once a policy is in the first stage **330** of a two stage commitment, it is effectively locked into the target **110**, merely awaiting the trigger signal to make the configuration change. The assignment step **310** of two stage deployment **300** is much more fluid and versatile. It has the advantage that it is visible to the user and can allow target-specific operations to be performed on the policy prior to commitment **320**.

Note that the policy-based network management system tracks objects corresponding to policies and targets **110**. Relationships between these object are also maintained: for a given target **110**, the system tracks what policy **120** is assigned and what policy **120** is committed. This is tracked by target **110** since the target **110** can have at most one policy **120** of a given policy type assigned and one committed. A given policy **120**, on the other hand, may be assigned to Target_1 and deployed on Target_2.

Figure 4A is a drawing of a system **400** for policy **120** management by a server program **410** for the target **110** as described in various representative embodiments of the present patent document. A console **430** connected to the server program **410** provides the user interface to enable the assignment of policy **120** to the appropriate targets **110** prior to commitment. The policy **120** is typically stored in a memory **445** located on a computer program storage medium **447** connected to the server program **410**, all of which could be located on a computer **405**.

Figure 4B is a drawing of another system **402** for policy **120** management by the server program **410** for the target **110** as described in various representative embodiments of the present patent document. In figure 4B, the server program **410** transfers policy **120** to a policy configuration agent **450** which in turn installs the policy **120** onto the target **110**. The policy configuration agent **450** translates the policy **120** as received from the server program **410** into policy **120** configuration specific to the target **110**. The policy configuration agent **450** is typically a software program operating on a computer on the network **220**.

Figure 5A is a flow chart of policy deployment **300** to the target **110** with one stage of policy commitment **320** as described in various representative embodiments of

the present patent document. In a manner similar to that of figure 3, in block 510 the server program 410 assigns policy 120 to the target 110. Block 510 then transfers control to block 520.

In block 520 the server program 410 activates policy 120 on the target 110. Activation is effected by the reconfiguration of the target 110 to reflect the policy 120. Reconfiguration could be effected by first clearing the old policy and then rewriting the new policy 120 into the target. Reconfiguration could also be effected by writing the new policy 120 over the old policy on the target.

Note that in one stage policy loading and activating policy 120 on the target 110 occurs as substantially one step.

Figure 5B is another flow chart of policy deployment 300 to the target 110 with one stage of policy commitment 320 as described in various representative embodiments of the present patent document. In a manner similar to that of figure 3, in block 515 the server program 410 assigns policy 120 to the target 110. Block 515 then transfers control to block 525.

In block 525 the server program 410 transfers policy 120 to the policy configuration agent 450. The policy configuration agent 450 translates the policy 120 as received from the server program 410 into policy 120 configuration specific to the target 110. Block 525 then transfers control to block 535.

In block 535 the policy configuration agent 450 activates policy 120 on the target 110. Activation is effected by the reconfiguration of the target 110 to reflect the policy 120. Reconfiguration could be effected by first clearing the old policy and then rewriting the new policy 120 into the target. Reconfiguration could also be effected by writing the new policy 120 over the old policy on the target.

Note that in one stage policy transfer of the policy 120 from the server program 410 to the policy configuration agent 450 and subsequent loading and activating policy 120 by the policy configuration agent 450 on the target 110 occurs as substantially without further user input.

Figure 6A is a flow chart of policy deployment 300 to the target 110 with two stage policy commitment 320 as described in various representative embodiments of the

present patent document. In a manner similar to that of figure 3, in block 610 the server program 410 assigns policy 120 to the target 110. Block 610 then transfers control to block 620.

In block 620 the server program 410 loads policy 120 on the target 110. Block 620 then transfers control to block 630.

In block 630 the server program 410 activates policy 120 on the target 110. Activation is effected by the reconfiguration of the target 110 to reflect the policy 120. Reconfiguration could be effected by first clearing the old policy and then rewriting the new policy 120 into the target. Reconfiguration could also be effected by writing the new policy 120 over the old policy on the target.

Figure 6B is another flow chart of policy deployment 300 to the target 110 with two stage policy commitment 320 as described in various representative embodiments of the present patent document. In a manner similar to that of figure 3, in block 615 the server program 410 assigns policy 120 to the target 110. Block 615 then transfers control to block 625.

In block 625 the server program 410 transfers policy 120 to the policy configuration agent 450. The policy configuration agent 450 translates the policy 120 as received from the server program 410 into policy 120 configuration specific to the target 110. Block 625 then transfers control to block 635.

In block 635 the policy configuration agent 450 loads policy 120 onto the target 110. Block 635 then transfers control to block 645.

In block 645 the server program 410 activates policy 120 on the target 110. Activation is effected by the reconfiguration of the target 110 to reflect the policy 120. Reconfiguration could be effected by first clearing the old policy and then rewriting the new policy 120 into the target. Reconfiguration could also be effected by writing the new policy 120 over the old policy on the target.

In another representative embodiment, the assigned policy 120 is retained by the policy configuration agent 450 until the command is received to activate the policy 120. At that time the policy 120 is loaded onto the target 110 and activated.

5. Summary of Operations - Two Stage Policy Commitment

The policy-based network management system supports a number of operations related to the two stage deployment mechanism. Figure 7 is a drawing of a block diagram of various operations that can be performed on the assigned policy **120**.

Operation **310** of figure 7, as in figure 3, assigns policy **120**. The system **400** allows the user to assign the policy **120** to the target **110** on a per target **110** basis, i.e., given the target **110**, present the list of possible policies **120** so that one can be assigned, or on a per policy **120** basis, i.e., given the policy **120**, present the list of targets **110** which support the policy's **120** type so the policy **120** can be assigned to one of them. This operation will create and store the assignment relationship based on the target **110** as described above.

Operation **710** of figure 7 displays assigned policy **120** for a given target **110**. The system **400** displays a list of targets **110**. For each target **110**, the system **400** displays its assigned policies **120** and committed policies **120**. This requires the system **400** to support finding the assignment relationship for a given target **110** so the policy **120** can be displayed.

Operation **720** of figure 7 tests/simulates assigned policy **120** for a given target **110**.

Operation **730** of figure 7 clears assigned policy **120** for a given target **110**. The system **400** allows the user to clear the assigned policy **120** for a given target **110**. In this case, the system clears the assigned policy **120** relationship for that target **110**.

Operation **740** of figure 7 determines to which targets **110** the policy **120** is assigned. The system **400** allows the user to see to which targets **110** a given policy **120** is assigned. This operation is supported by a query which searches through the assignment relationships for entries which include a reference to the given policy **120**.

Operation **320** of figure 7, as in figure 3, commits assigned policy **120** for the given target **110**. The system **400** allows the user to commit the assigned policy **120** on the given target **110**. This operation moves the assigned policy **120** into the committed state on the target **110**, overwriting the target's **110** previously committed policy **120** and clearing the target's **110** assigned policy **120**. This operation affects both the stored

relationships for the target **110**, i.e., assigned and committed policy **120**, as well as the target's **110** configuration, i.e., changing the installed policy **120** on the target **110**. Differences between one stage and two stage commitment have been previously described.

6. Concluding Remarks

Primary advantages of the embodiment as described in the present patent document over prior methods for deploying policy are the ability to overcome the problem that policies **120** may be programmed into the target **110** which may be subsequently rejected due to policy **120** inconsistencies and other reasons and the ability to perform target specific operations such as testing and simulation of policy prior to commitment.

While the present invention has been described in detail in relation to preferred embodiments thereof, the described embodiments have been presented by way of example and not by way of limitation. It will be understood by those skilled in the art that various changes may be made in the form and details of the described embodiments resulting in equivalent embodiments that remain within the scope of the appended claims.

CLAIMS

What is claimed is:

1. A computer implemented method for deploying a policy **[120]** to a target **[110]**, comprising the steps of:

assigning the policy **[120]** to the target **[110]**, providing the policy **[120]** specifies conditional action implementable on the target **[110]**, providing the target is a resource on a network **[220]**, and providing policy **[120]** assignment comprises association of the policy **[120]** with the target **[110]** prior to policy **[120]** reconfiguration of the target **[110]**; and

activating the policy **[120]** on the target **[110]**, providing the policy **[120]** has been activated when target **[110]** actions comply with the policy **[120]**.

2. The computer implemented method as recited in claim 1, providing the target **[110]** is selected from the group consisting of an electronic device **[230]**, an interface **[110]** of the electronic device **[230]**, a function implementable on the interface **[110]** of the electronic device **[230]**, a software program **[110]**, and a function implementable in the software program **[110]**.

3. A computer implemented method for deploying a policy **[120]** to a target **[110]**, comprising the steps of:

assigning the policy **[120]** to the target **[110]**, providing the policy **[120]** specifies conditional action implementable on the target **[110]**, providing the target is a resource on a network **[220]**, and providing policy **[120]** assignment comprises association of the policy **[120]** with the target **[110]** prior to policy **[120]** reconfiguration of the target **[110]**;

loading the policy **[120]** onto the target **[110]** prior to policy **[120]** activation on the target **[110]**; and

activating the policy **[120]** on the target **[110]**, providing the policy **[120]** has been activated when target **[110]** actions comply with the policy **[120]**.

4. The computer implemented method as recited in claim 3, providing:

the method step of loading the policy **[120]** onto the target **[110]** further comprises the steps of:

transferring the policy **[120]** from a server program **[410]** to a policy configuration agent **[450]**, wherein the policy configuration agent **[450]** has capability of translating the policy **[120]** as received from the server program **[410]** into policy **[120]** configuration specific to the target **[110]**;

translating the policy **[120]** by the policy configuration agent **[450]** as received from the server program **[410]** into policy **[120]** configuration specific to the target **[110]**; and

loading the policy [120] onto the target [110] by the policy configuration agent [450]; and

the method step of assigning policy [120] further comprises association of the policy [120] with the target [110] prior to transfer of the policy [120] to the policy configuration agent [450].

5. The computer implemented method as recited in claim 3, providing the target [110] is selected from the group consisting of an electronic device [230], an interface [110] of the electronic device [230], a function implementable on the interface [110] of the electronic device [230], a software program [110], and a function implementable in the software program [110].

6. A computer program storage medium [447] readable by a computer, tangibly embodying a computer program of instructions executable by the computer to perform method steps, the method steps comprising:

assigning a policy [120] to a target [110], providing the policy [120] specifies conditional action implementable on the target [110], providing the target is a resource on a network [220], and providing policy [120] assignment comprises association of the policy [120] with the target [110] prior to policy [120] reconfiguration of the target [110]; and

activating the policy [120] on the target [110], providing the policy [120] has been activated when target [110] actions comply with the policy [120].

7. The computer program storage medium [447] as recited in claim 6, wherein the target [110] is selected from the group consisting of an

electronic device [230], an interface [110] of the electronic device [230], a function implementable on the interface [110] of the electronic device [230], a software program [110], and a function implementable in the software program [110].

8. A computer program storage medium [447] readable by a computer, tangibly embodying a computer program of instructions executable by the computer to perform method steps, the method steps comprising:

assigning a policy [120] to a target [110], providing the policy [120] specifies conditional action implementable on the target [110], providing the target is a resource on a network [220], and providing policy [120] assignment comprises association of the policy [120] with the target [110] prior to policy [120] reconfiguration of the target [110];

loading the policy [120] onto the target [110] prior to policy [120] activation on the target [110]; and

activating the policy [120] on the target [110], providing the policy [120] has been activated when target [110] actions comply with the policy [120].

9. The computer program storage medium [447] as recited in claim 8, providing:

the method step of loading the policy [120] onto the target [110] further comprises the method steps of:

transferring the policy [120] from a server program [410] to a policy configuration agent [450], wherein the policy configuration

agent [450] has capability of translating the policy [120] as received from the server program [410] into policy [120] configuration specific to the target [110];

translating the policy [120] by the policy configuration agent [450] as received from the server program [410] into policy [120] configuration specific to the target [110]; and

loading the policy [120] onto the target [110] by the policy configuration agent [450]; and

the method step assigning policy [120] further comprises the method step of associating the policy [120] with the target [110] prior to transfer of the policy [120] to the policy configuration agent [450].

10. The computer program storage medium [447] as recited in claim 8, wherein the target [110] is selected from the group consisting of an electronic device [230], an interface [110] of the electronic device [230], a function implementable on the interface [110] of the electronic device [230], a software program [110], and a function implementable in the software program [110].

Application No: GB 0100126.2
Claims searched: 1-10

Examiner: Keith Sylvan
Date of search: 29 October 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): H4K (KF42, KFMA)

Int Cl (Ed.7): H04Q (3/00)

Other: Online: WPI,JAPIO,EPODOC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A,E	GB2356316 A	H.P. See the abstract.	-
A	GB2337409 A	Firsttel. See the abstract.	-

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.